Notice of Allowability	Application No. 10/017,230	Applicant(s) PETERSEN ET AL.	
	Examiner Kristin D. Sandoval	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *communications filed May 22, 2006*.

2. ☒ The allowed claim(s) is/are *1-57 and 69-134*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 6/20/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. John Castellano on August 2, 2006 and August 3, 2006.

The application has been amended as follows:

Due to the cancellation of claims 58-68 and the dependency of earlier claims depending on later claims, the claims have been renumbered, along with the changes in their dependencies. In addition, claims 56 and 57 have also been amended.

See and enter attached Examiners Amendment.

The following is an examiner's statement of reasons for allowance:

Regarding claim 118:

Amendments to the claims overcome the prior art rejections made in the previous action. The prior art of record (Crandall, U.S. 6,587,563) discloses a mathematical system expressed in discrete terms where at least one variable is an integer and performing computations on the variable in order to produce a resulting number to obtain an output of a cryptographic system. Crandall fails to teach the use of an imaginary decimal separator placed within the integer number in order to represent the integer as a real number and positioning the imaginary decimal

separator in the resulting number at a predetermined position by either correcting the position of the imaginary decimal separator or placing an imaginary separator in the resulting number.

None of the other references cited in the prior action combine with Crandall to disclose the limitations.

An updated search did not uncover any new prior art not owned by the same assignee of the instant application. No art disclosing, nor motivation to combine has been found which recites using an imaginary decimal separator placed within the integer number in order to represent the integer as a real number and positioning the imaginary decimal separator in the resulting number at a predetermined position by either correcting the position of the imaginary decimal separator or placing an imaginary separator in the resulting number.

All other pending claims are dependent on allowable claim 118 and are allowable for that reason.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin D. Sandoval whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
PRIMARY EXAMINER

Kristin D Sandoval
Examiner
Art Unit 2132

KDS

AMENDMENTS TO THE CLAIMS

The following is a complete listing of revised claims with a status identifier in parenthesis.

LISTING OF CLAIMS

~~1~~2. The method of claim ~~1181~~, wherein the integer number is a fixed-point number,

- performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtaining, from said computations, the resulting number, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

the method further comprising:

- extracting a set of data which represents at least one of:
- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

~~2~~3. A method according to claim ~~1~~2, wherein said set of data represent a pseudo-random number.

~~3~~4. A method according to claim ~~1~~2, wherein said computations include at least a first and a second fixed-point number, each fixed-point number having a decimal separator, wherein the decimal separator of the first fixed-point number is positioned at a position different from the position of the decimal separator of the second fixed-point number.

45. A method according to claim ~~3~~4, wherein the step of performing computations includes positioning the decimal separator of the first and second fixed-point number at selected positions.

~~5~~6. A method according to claim ~~1~~2, wherein said at least one function is non-linear.

~~6~~7. A method according to claim ~~1~~2, wherein the resulting number is expressed as a variable selected from the group consisting of:

- an integer number,
- a floating point number, and
- a fixed-point number.

~~7~~8. A method according to claim ~~1~~2, wherein the mathematical system comprises at least one of:

- a differential equation,
- a discrete mapping.

~~8~~9. A method according to claim ~~7~~8, wherein the differential equation comprises at least one of:

- a partial differential equation,
- an ordinary differential equation.

~~9~~10. A method according to claim ~~7~~8, wherein the discrete mapping comprises at least one of:

- an area-preserving map,
- a non area-preserving map.

~~10~~11. A method according to claim ~~7~~8, wherein the mathematical system comprises at least one non-linear function governing at least one state variable X.

~~11~~12. A method according to claim ~~10~~11, wherein the mathematical system comprises a set of non-linear mapping functions.

~~12~~13. A method according to claim ~~9~~10, wherein the map comprises at least one of:

- a logistic map of the form:

  $x_{n+1}=\mu x_n(1-x_n)$,

– an Anosov map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1,$$

– a Hénon map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 + y_n - ax_n^2 \\ bx_n \end{bmatrix}.$$

~~13~~14 A method acco rding to claim ~~1~~2, wherein the mathematical system comprises at least one non-linear differential equation.

~~14~~15. A method according to claim ~~13~~14, wherein the mathematical system comprises a set of non-linear differential equations.

~~15~~16. A method according to claim ~~7~~8, wherein the mathematical system has at least one positive Lyapunov exponent.

~~16~~17. A method according to claim ~~7~~8, comprising computing at least one Lyapunov exponent at least once during the mathematical computations.

~~17~~18. A method according to claim ~~13~~14, wherein the at least non-linear differential equation governs at least one state variable, X, which is a function of at least one independent variable, t.

~~18~~19. A method according to claim ~~14~~15, wherein the set of non-linear differential equations is a Lorenz system.

~~19~~20. A method according to claim ~~18~~19, wherein the Lorenz system consists of the following differential equations:

$$\frac{dx}{dt} = \sigma(y - x),$$

$$\frac{dy}{dt} = rx - y - xz,$$

$$\frac{dz}{dt} = xy - bz,$$

wherein X=(x, y, z) are state variables, t is the independent variable, and σ, r and b are parameters.

~~20~~21. A method according to claim ~~13~~14, wherein the step of performing computations comprises numerically integrating at least one of:

- the non-linear differential equation, and
- the non-linear differential equations of said set of non-linear differential equations,

by repeatedly computing a solution X_{n+1} based on at least one previous solution X_m, $m \leq n+1$, and a step length, ΔTn, of the independent variable, t.

~~21~~22. A method according to claim ~~20~~21, wherein the step of integrating comprises providing at least one initial condition, X_0, of the state variable, X, and an initial step length, ΔT_0.

~~22~~23. A method according to claim ~~10~~11, wherein the step of performing computations comprises numerically iterating the non-linear mapping function.

~~23~~24. A method according to claim ~~22~~23, wherein the step of iterating comprises providing at least one initial condition, X_0, of the state variable, X.

~~24~~25. A method according to claim ~~20~~21, wherein, in the discretized formulation of the Lorenz system, the solution X_{n+1} is computed using the step length $\Delta T=(\Delta t_{x,n}, \Delta t_{y,n}, \Delta t_{z,n})$ as follows:

$$x_{n+1} = x_n + (\sigma(y_n - x_n)) \cdot \Delta t_{x,n}$$
$$y_{n+1} = y_n + (x_n(r - z_n) - y_n) \cdot \Delta t_{y,n}$$
$$z_{n+1} = z_n + (x_n y_n - b z_n) \cdot \Delta t_{z,n},$$

wherein:

$\Delta t_{x,n}$ is the step length used in the computation of x_{n+1},

$\Delta t_{y,n}$ is the step length used in the computation of y_{n+1},

$\Delta t_{z,n}$ is the step length used in the computation of z_{n+1}.

~~25~~26. A method according to claim ~~20~~21, wherein the step length ΔT is constant throughout the computations.

~~26~~27. A method according to claim ~~20~~21, wherein, in each integration step, at least one of the elements ($\Delta t_{x,n}$, $\Delta t_{y,n}$, $\Delta t_{z,n}$) of the step length ΔT is a function of at least one number related to said computations.

~~27~~28. A method according to claim ~~26~~27, wherein, in each integration step, at least one of the elements ($\Delta t_{x,n}$, $\Delta t_{y,n}$, $\Delta t_{z,n}$) of the step length ΔT is a function of at least one solution, X_m, which is a solution to the mathematical system.

~~28~~29. A method according to claim ~~26~~-27 wherein, in each integration step, at least one of the elements ($\Delta t_{x,n}$, $\Delta t_{y,n}$, $\Delta t_{z,n}$) of the step length ΔT is a function of at least one given step length, ΔT_m.

~~29~~30. A method according to claim ~~1~~2, wherein a key selected from an encryption key and a decryption key is used to determine at least one value of at least one variable in the mathematical system.

~~30~~31. A method according to claim ~~29~~30, wherein the key is used to determine at least a part of the initial condition X_0.

~~31~~32. A method according to claim ~~29~~30, wherein the key is used to determine at least a part of the initial step length ΔT_0.

~~32~~33. A method according to claim ~~29~~30, wherein the key is used to determine the at least a part of at least one of the parameters.

~~33~~34. A method according to claim ~~29~~30, wherein the key is a public key.

~~34~~35. A method according to claim ~~29~~30, wherein the key is a private key.

~~35~~36. A method according to claim ~~1~~2, comprising extracting a plurality of numbers resulting from the computations.

~~36~~37. A method according to claim ~~1~~2, wherein the step of extracting comprises extracting at least one number derived from k bits of the resulting number.

~~37~~38. A method according to claim ~~1~~2, wherein the step of extracting comprises extracting the k least significant bits of the resulting number.

~~38~~39. A method according to claim ~~36~~37, wherein k is a value selected from the group consisting of: 8, 16, 32, 64, and 128.

~~39~~40. A method according to claim ~~36~~37, wherein a plurality of numbers are extracted.

~~40~~41. A method according to claim ~~1~~2, wherein the extracted set of data is manipulated by means of at least one of:

- an arithmetic operation, and
- a logical operation,

so as to obtain a combined set of data.

~~41~~42. A method according to claim ~~40~~41, wherein at least one of the:

- extracted set of data, and
- the combined set of data

is combined with original data, so as to encrypt the original data.

~~42~~43. A method according to claim ~~40~~41, wherein at least one of:

- extracted set of data, and
- the combined set of data

is combined with encrypted data, so as to decrypt the encrypted data and obtain the original data.

~~43~~44. A method according to claim ~~40~~41, wherein the combining of data comprises an XOR operation.

~~44~~45. A method according to claim ~~1~~2, wherein said computations include data representing a block of plaintext in a block-cipher encryption and decryption system.

~~45~~46. A method according to claim ~~1~~2, wherein the extracted set of data is used to define at least one operation on a block of plaintext in a block-cipher encryption and decryption system.

~~46~~47. A method according to claim ~~41~~42, wherein the combining of data comprises addition of the original data and the combined set of data for encryption, and subtraction of the combined set of data from the encrypted data for decryption.

~~47~~48. A method according to claim ~~41~~42, wherein the combining of data comprises subtraction of the combined set of data from the original data for encryption, and addition of the combined set of data and the encrypted data for decryption.

~~48~~49. A method according to claim ~~1~~2, wherein the extracted set of data is used as at least one of: an encryption key and a decryption key.

~~49~~50. A method according to claim ~~1~~2, wherein the extracted set of data is used to generate at least one of: an encryption key and a decryption key.

~~50~~51. A method according to claim ~~1~~2, wherein the extracted set of data is used in generation of data representing a digital signature.

~~51~~52. A method according to claim ~~1~~2, wherein the extracted set of data is used in watermarking of digital data.

~~52~~53. A method according to claim ~~1~~2, wherein the computations are performed on an electronic device which comprises an electronic processing unit having a register width, the method comprising the steps of:

- expressing at least one integer number of a bit width larger than said register width as at least two sub-numbers each having a bit width which is at most equal to said register width,
- performing at least one of said computations as a sub-computation on each of the sub-numbers so as to arrive at at least two partial results, expressed as integer numbers of a bit width smaller which is at most equal to the register width of the processing unit,
- concatenating the partial results to yield a representation of a result of said at least one computation.

~~53~~54. A computer program for performing the method of claim ~~1181~~, wherein the integer number is a fixed-point number, the computer program being adapted to:

- perform said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtain, from said computations, the resulting number, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

the computer program being further adapted to:

- extract a set of data which represents at least one of:
- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

~~54~~55. A computer readable data carrier loaded with a computer program for performing the method of claim ~~1181~~, wherein the integer number is a fixed-point number, the computer program being adapted to:

- perform said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtain, from said computations, the resulting number, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

the computer program being further adapted to:

- extract a set of data which represents at least one of:
- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

~~55~~56. A computer which is operatively connected to a computer readable data carrier loaded with a computer program for performing the method of claim ~~11~~81, wherein the integer number is a fixed-point number, the computer program being adapted to:

- perform said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtain, from said computations, the resulting number, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

the computer program being further adapted to:

- extract a set of data which represents at least one of:
- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number,

wherein the computer comprises processor means for running said program.

~~56~~57. ~~A signal comprising~~ ~~an~~ An extracted set of data which have been derived from the method of claim ~~11~~81, wherein the integer number is a fixed-point number,

- said computations have been performed in such a way that the computations have included the at least one variable expressed as a fixed-point number,
- the resulting number has been obtained from said computations, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

whereby the extracted set of data represents at least one of:

- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

~~57~~58. ~~A signal comprising an~~ An encrypted set of data which has been derived as a combination of plaintext and at least one set of data extracted from computations in accordance with the method of claim ~~1181~~, wherein the integer number is a fixed-point number,

- said computations have been performed in such a way that the computations have included the at least one variable expressed as a fixed-point number,
- the resulting number has been obtained from said computations, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

whereby the extracted set of data represents at least one of:

- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

~~58 - 68. (Canceled)~~

~~69~~59. A method of generating a pseudo-random number, the method comprising:
performing the method of claim ~~1181~~;

II) defining a seed value representing at least an initial condition for the mathematical system, wherein the integer number is a fixed-point number,

IV) performing said computations in an electronic device, the computations including the at least one variable expressed as a fixed-point number and obtaining, from said computations, a resulting number, the resulting number representing at least one of:

a. at least a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system,

V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations.

~~70~~60. A method according to claim ~~69~~59, wherein the pseudo-random number is extracted as a number derived from k digits of said at least one number which has occurred during the computations.

~~71~~61. A method according to claim ~~70~~60, wherein the pseudo-random number is extracted as a number derived from the k least significant digits of said at least one number.

~~72~~62. A method according to claim ~~69~~59, the method comprising the steps of repeating steps IV) and V) until a given amount of pseudo-random numbers has been generated.

~~73~~63. A method according to claim ~~69~~59, wherein a given amount of pseudo-random numbers is generated and stored in a memory of the electronic device as a spare seed value.

~~74~~64. A method according to claim ~~69~~59, wherein a plurality of resulting numbers are obtained which represent at least parts of solutions to the mathematical system, the method further comprising detecting periodic behavior in the solution of the mathematical system, the mathematical system comprising at least one non-linear function governing at least one state variable with respect to at least one independent variable, the detecting of periodic behavior comprising:

variable with respect to at least one independent variable, the detecting of periodic behavior comprising:

- storing selected solutions in an array, A, in a memory of the electronic device, the array being adapted to store a finite number, n+1, of solutions,
- determining whether at least one of:
- a current solution, and
- a particular one of said solutions stored in the array

is substantially identical to another solution stored in the array,

the method further comprising:

if the step of determining reveals that at least one of

- the current solution, and
- the particular solution

is identical to another solution:

interrupting the pseudo-random-number generation, i.e. interrupting repetition of steps IV) and V),

using the spare seed value as the seed value in the step II),

resuming the pseudo-random-number generation, i.e. resuming repetition of steps IV) and V).

~~75~~65. A method according to claim ~~74~~64, further comprising, prior to the step of resuming the pseudo-random number generation, generating and storing, in a memory of the electronic device, a given amount of pseudo-random numbers as a new spare seed value.

~~76~~66. A method according to claim ~~69~~59, wherein each level in the array, A, is reset prior to step IV), when steps IV) and V) are initiated with a new seed value at step II).

~~77~~67. A method of encrypting a set of original data into a set of encrypted data, the method comprising the steps of:

A) generating a pseudo-random number by performing the method of claim ~~11~~81;

V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,

B) manipulating the original data and the pseudo-random number by means of at least one of:
i. an arithmetic operation, and
ii. a logical operation,
so as to obtain a combined set of data, the combined set of data being the encrypted data.

~~78~~68. A method according to claim ~~77~~67, wherein, prior to step A), a sub-set of the original data is separated from the set of data, and wherein step B) is performed on the sub-set of data.

~~79~~69. A method according to claim ~~77~~67, wherein the pseudo-random number is extracted as a number derived from k digits of said at least one number which has occurred during the computations.

~~80~~70. A method according to claim ~~77~~67, wherein the pseudo-random number is extracted as a number derived from the k least significant digits of said at least one number which has occurred during the computations.

~~81~~71. A method according to claim ~~77~~67, the method comprising the steps of repeating steps IV) and V) until a given amount of pseudo-random numbers has been generated.

~~82~~72. A method according to claim ~~77~~67, wherein a given amount of pseudo-random numbers is generated and stored in a memory of the electronic device as a spare encryption key.

~~83~~73. A method according to claim ~~82~~72, wherein a plurality of resulting numbers are obtained which represent at least parts of solutions to the mathematical system, the method further comprising detecting periodic behavior in the solution of the mathematical system, the mathematical system comprising at least one non-linear function governing at least one state variable with respect to at least one independent variable, the detecting of periodic behavior comprising:

- storing selected solutions in an array, A, in a memory of the electronic device, the array being adapted to store a finite number, n+1, of solutions,

– determining whether at least one of:
– a current solution, and
– a particular one of said solutions stored in the array
is substantially identical to another solution stored in the array,
the method further comprising:
if the step of determining reveals that at least one of:
– the current solution, and
– the particular solution
is identical to another solution:
– interrupting the pseudo-random number generation, i.e. interrupting repetition of steps IV) and V),
– using the spare encryption key as the encryption key in step II),
– resuming the pseudo-random number generation, i.e. resuming repetition of steps IV) and V).

~~84~~74. A method according to claim ~~83~~73, further comprising, prior to the step of resuming the pseudo-random number generation, generating and storing, in a memory of the electronic device, a given amount of pseudo-random numbers as a new spare encryption key.

~~85~~75. A method according to claim ~~77~~67, wherein each level in the array, A, is reset prior to step IV), when steps IV) and V) are initiated with a new seed value at step II).

~~86~~76. A method of decrypting a set of encrypted data which has been encrypted by a method of encrypting a set of original data into said set of encrypted data, the method of encrypting comprising the steps of:
A) generating a pseudo-random number by performing the method of claim ~~11~~81;
V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,
B) manipulating the original data and the pseudo-random number by means of at least one of:
i. an arithmetic operation, and
ii. a logical operation,

so as to obtain a combined set of data, the combined set of data being the encrypted data,
the method of decrypting comprising the steps of:
a) performing step A), so as to extract the same pseudo-random number as extracted in step V),
b) manipulating the encrypted data and the pseudo-random number by means of at least one of:
- an arithmetic operation, and
- a logical operation,

so as to obtain the original, decrypted, version of the data.

~~87~~77. A method according to claim ~~86~~76, wherein, prior to step a), a sub-set of the encrypted data is separated from the set of encrypted data, the method of decrypting comprising performing steps a) and b) on said sub-set of data.

~~88~~78. A method according to claim ~~87~~77 comprising repeating the steps A)-B) until a plurality of sub-sets which in common constitute the entire set of encrypted data have been decrypted.

~~89~~79. A computer program for encrypting and decrypting a set of data, the computer program being adapted to run in an encryption mode and in a decryption mode; the computer program being further adapted to:
- i) generate a pseudo-random number in a reproducible way by performing the method of claim ~~1181~~, wherein the integer number is a fixed-point number,
- performing computations including the at least one variable expressed as a fixed-point number,
- obtaining, from the computations, the resulting number, the resulting number representing at least one of:

a. a part of a solution to the mathematical system, and
b. a number usable in further computations involved in the numerical solution of the mathematical system,
- extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,

ii) manipulate the data and the pseudo-random number by means of at least one of:

- an arithmetic operation, and
- a logical operation,

so as to obtain a combined set of data, wherein:

- the combined set of data represents an encrypted version of the data in case the computer program is run in encryption mode,
- the combined set of data represents a decrypted version of the data in case the computer program is run in decryption mode.

~~90~~80. A computer readable data carrier loaded with a computer program for encrypting and decrypting a set of data, the computer program being adapted to run in an encryption mode and in a decryption mode, the computer program being further adapted to:

- i) generate a pseudo-random number in a reproducible way by performing the method of claim ~~11~~81, wherein the integer number is a fixed-point number,
- performing computations including the at least one variable expressed as a fixed-point number,
- obtaining, from the computations, the resulting number, the resulting number representing at least one of:

a. a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system,

- extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,

ii) manipulate the data and the pseudo-random number by means of at least one of:

- an arithmetic operation, and
- a logical operation,

so as to obtain a combined set of data, wherein:

- the combined set of data represents an encrypted version of the data in case the computer program is run in encryption mode,

the combined set of data represents a decrypted version of the data in case the computer program is run in decryption mode.

~~91~~81. A computer being operatively connected to a computer readable data carrier loaded with a computer program for encrypting and decrypting a set of data, the computer program being adapted to run in an encryption mode and in a decryption mode, the computer program being further adapted to:

- i) generate a pseudo-random number in a reproducible way by performing the method of claim ~~1181~~, wherein the integer number is a fixed-point number,
- performing computations including the at least one variable expressed as a fixed-point number,
- obtaining, from the computations, the resulting number, the resulting number representing at least one of:

a. a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system,

- extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,

ii) manipulate the data and the pseudo-random number by means of at least one of:

- an arithmetic operation, and
- a logical operation,

so as to obtain a combined set of data, wherein:

- the combined set of data represents an encrypted version of the data in case the computer program is run in encryption mode,

the combined set of data represents a decrypted version of the data in case the computer program is run in decryption mode,

the computer comprising processor means for running said program.

~~92~~82. A method according to claim ~~69~~79, further comprising:

performing steps I) - V) in a plurality of instances in parallel.

~~93~~83. A method according to claim ~~92~~82, comprising transmitting data between the plurality of instances at least while performing step IV) for each of the instances.

~~94~~84. A method according to claim ~~92~~82, further comprising transmitting data between the plurality of instances while performing step V) for each of the instances.

~~95~~85. A method according to claim ~~92~~82, comprising combining, by use of at least one of:

- an arithmetic operation, and
- a logical operation,

a plurality of pseudo-random numbers extracted at step V) in each of the instances into a common pseudo-random number.

~~96~~86. The method of claim ~~11~~81, wherein the integer number is a fixed-point number,

- performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtaining, from said computations, a resulting number, the resulting number representing at least one of:

a. at least a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system,

the step of performing computations comprising:

- repeatedly computing a solution X_{n+1} based on at least one previous solutions X_m, $m \leq n+1$, whereby the step of performing computations is initiated based on at least one initial condition, X_0, of the state variable, X,

the method further comprising:

- providing a cryptographic key as an input to said computations, whereby the cryptographic key is used in generation of the initial condition X_0.

~~97~~87. A method of determining an identification value for identifying a set of data, the method comprising performing as the method of claim ~~11~~81, wherein the integer number is a fixed-point number,

- performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtaining, from said computations, the resulting number, the resulting number representing at least one of:

a. at least a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system,

whereby a representation of at least part of the set of data is used in said computations, the method further comprising:

- extracting, as said identification value, at least a part of said resulting number.

~~98~~88. A method according to claim ~~97~~87, wherein a cryptographic key is used as a seed value for the computations.

~~99~~89. A method according to claim ~~97~~87, wherein the mathematical system comprises at least one of:

- a differential equation,
- a discrete mapping.

~~100~~90. A method according to claim ~~99~~89, wherein the differential equation comprises at least one of:

- a partial differential equation,
- an ordinary differential equation.

~~101~~91. A method according to claim ~~99~~89, wherein the discrete mapping comprises at least one of:

- an area-preserving map,

– a non area-preserving map.

~~102~~92. A method according to claim ~~99~~89, wherein the mathematical system comprises at least one non-linear function governing at least one state variable X.

~~103~~93. A method according to claim ~~102~~92, wherein the non-linear mapping function comprises a logistic map of the form $x_{n+1}=\lambda x_n(1-x_n)$, wherein λ is a parameter, x_{n+1} is the value of state variable x at the (n+1)'th stage in the computations, and x_n is the value of state variable x at the n'th stage in the computations.

~~104~~94. A method according to claim ~~103~~93, wherein the logistic map is modified into the form $x_{n+1}=\lambda x_n(1-x_n)+\varepsilon(x_n-m_n)$, wherein λ and ε are parameters, x_{n+1} is the value of state variable x at the (n+1)'th stage in the computations, x_n is the value of state variable x at the n'th stage in the computations, and m_n contains a representation of an n'th portion of the set of data.

~~105~~95. A method according to claim ~~103~~93, wherein a cryptographic key is used for at least partially determining at least one of the following: λ, ε and an initial value x_0 of state variable x.

~~106~~96. A method according to claim ~~97~~87, wherein the mathematical system comprises a set of non-linear mapping functions.

~~107~~97. A method according to claim ~~106~~96, wherein the set of mapping functions comprises at least one of:

– an Anosov map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1,$$

– a Hénon map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 + y_n - ax_n^2 \\ bx_n \end{bmatrix}.$$

~~10898~~. A method according to claim ~~9787~~, wherein the mathematical system comprises at least one non-linear differential equation.

~~10999~~. A method according to claim ~~10898~~, wherein the mathematical system comprises a set of non-linear differential equations.

~~110~~100. A method according to claim ~~9787~~, wherein the mathematical system has at least one positive Lyapunov exponent.

~~111~~101. A method according to claim ~~9787~~, comprising computing at least one Lyapunov exponent at least once during the mathematical computations.

~~112~~102. A method according to claim ~~10898~~, wherein the at least one non-linear differential equation governs at least one state variable, X, which is a function of at least one independent variable, t.

~~113~~103. A method according to claim ~~10999~~, wherein the set of non-linear differential equations comprises a Lorenz system.

~~114~~104. The method of claim ~~1181~~, further comprising:

- restricting the range of at least a selected variable of said function, so as to exclude values which the selected variable, by virtue of said function, would assume if not restricted by said range,
- performing said computations so as to obtain the resulting number, the resulting number representing at least one of:

a. a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system,

- when the computations result in a value for the selected variable which is beyond the range, assigning a value within the range to the selected variable.

~~115~~105. A method according to claim ~~114~~104, wherein the method is a part of a pseudo-random number generating method.

~~116~~106. A method according to claim ~~115~~105, wherein the pseudo-random number generating method generates pseudo-random numbers for use in at least one of encryption and decryption.

~~117~~107. A method according to claim ~~114~~104, wherein the mathematical system has at least one positive Lyapunov exponent.

~~118~~1. A method of performing numerical computations in a cryptographic system, which includes a mathematical system comprising at least one function, the method comprising the steps of:

- expressing the mathematical system in discrete terms,
- expressing at least one variable of the mathematical system as an integer number,
- placing an imaginary decimal separator in said integer number, whereby the integer number represents a real number,
- performing computations including the at least one variable expressed as an integer number so as to obtain a resulting number, the resulting number being expressed as an integer number,
- positioning the imaginary decimal separator in the resulting number at a predetermined position by performing at least one of the steps of:
- correcting the position of the imaginary decimal separator in the integer number, and
- placing an imaginary separator in the resulting number,

the method further comprising the step of using the resulting number to obtain an output of the cryptographic system.

~~119~~108. The method of claim ~~118~~1, wherein the integer number is a fixed-point number,

- performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,

- obtaining, from said computations, the resulting number, the resulting number representing at least one of:

a. at least a part of a solution to the mathematical system, and

b. a number usable in further computations involved in the numerical solution of the mathematical system.

~~120~~109. The method according to claim ~~69~~59, wherein the pseudo random number represents at least one of:

- i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

~~121~~110. The method according to claim ~~120~~109, wherein the pseudo-random number is extracted as a number derived from the k least significant digits of said at least one number.

~~122~~111. The method according to claim ~~120~~109, wherein said computations involve at least a first and a second fixed-point number, each fixed-point number having a decimal separator, wherein the decimal separator of the first fixed-point number is positioned at a position different from the position of the decimal separator of the second fixed-point number.

~~123~~112. The method according to claim ~~120~~109, wherein the mathematical system comprises a discrete mapping, comprising at least one of:

- a logistic map of the form:

  $x_{n+1}=\mu x_n(1-x_n)$,

- an Anosov map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1,$$

- a Hénon map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 + y_n - ax_n^2 \\ bx_n \end{bmatrix}.$$

~~124~~113. The method according to claim ~~120~~109, wherein the mathematical system comprises at least one of:

- a differential equation,
- a discrete mapping,

and wherein the mathematical system has at least one positive Lyapunov exponent.

~~125~~114. The method according to claim ~~120~~109, wherein the mathematical system comprises a set of non-linear differential equations, which set is a Lorenz system consisting of the following differential equations:

$$\frac{dx}{dt} = \sigma(y - x),$$
$$\frac{dy}{dt} = rx - y - xz,$$
$$\frac{dz}{dt} = xy - bz,$$

wherein X=(x, y, z) are state variables, t is the independent variable, and σ, r and b are parameters.

~~126~~115. The method according to claim ~~120~~109, wherein the mathematical system comprises at least one non-linear differential equation, wherein:

- the step of performing computations comprises numerically integrating the at least one non-linear differential equation by repeatedly computing a solution X_{n+1} based on at least one previous solution X_m, $m \leq n+1$, and a step length, ΔTn, of the independent variable, t, and wherein
- in each integration step, at least one of the elements ($\Delta t_{x,n}$, $\Delta t_{y,n}$, $\Delta t_{z,n}$) of the step length ΔT is a function of at least one number related to said computations.

~~127~~116. The method according to claim ~~120~~109, wherein a key selected from an encryption key and a decryption key is used to determine at least one value of at least one variable in the mathematical system.

~~128~~117. The method according to claim ~~127~~116, wherein the mathematical system includes at least one parameter, an initial condition X_0, and an initial step length ΔT_0, and wherein the key is used to determine at least one of:

- at least a part of the initial condition X_0,
- at least a part of the initial step length ΔT_0, and
- at least a part of said at least one parameter.

~~129~~118. The method according to claim ~~121~~110, wherein said step of extracting comprises extracting a plurality of numbers.

~~130~~119. The method according to claim ~~120~~109, wherein the extracted number is manipulated by means of at least one of:

- an arithmetic operation, and
- a logical operation,

so as to obtain a combined set of data.

~~131~~120. The method according to claim ~~130~~119, wherein at least one of:

- the extracted set of data, and
- the combined set of data

is used for at least one of:

- encryption of original data to obtain encrypted data, and
- decryption the encrypted data to obtain the original data.

~~132~~121. The method according to claim ~~120~~109, wherein the extracted number is used to generate at least one of: an encryption key and a decryption key.

~~133~~122. The method according to claim ~~120~~109, the method comprising performing steps I) - V) in a plurality of instances in parallel and transmitting data between the plurality of instances at least while performing at least one of steps IV) and V) for each of the instances.

~~134~~123. The method according to claim ~~133~~122, comprising combining, by use of at least one of:

- an arithmetic operation, and
- a logical operation,

a plurality of pseudo-random numbers extracted at step V) in each of the instances into a common pseudo-random number.